CLAIMS

What is claimed is:

1. (Original) A method implemented in a computing device of obtaining a password from a user, said method comprising:

storing authentication indicia recognized by said user in said computing device; and

prompting a user to enter said password by displaying a password entry screen containing said authentication indicia.

2. (Original) The method of claim 1 wherein storing authentication indicia recognized by said user in said computing device comprises storing said authentication indicia in a security module.

3. (Original) The method of claim 1 wherein displaying said password entry screen containing said authentication indicia comprises displaying said authentication indicia for a limited time.

4. (Original) The method of claim 1 further comprising obtaining said authentication indicia from said user.

5. (Original) The method of claim 1 further comprising halting programs running on said computing device not necessary for inputting said password while said password entry screen is displayed.

6. (Currently Amended) A method implemented by a security module in a computing device of obtaining a password from a user, said method comprising:

prompting a user to enter said password by displaying a password entry screen on a display;

halting programs not needed by said security module while said password entry screen is displayed;

obtaining said password from said user;

removing said password entry screen from said display; and

restarting halted programs after said password entry screen is removed from said display.

7. (Original) The method of claim 6 wherein halting programs not needed by said security module while said password entry screen is displayed comprises inhibiting an operating system in said computing device from responding to interrupts not associated with said security module.

8. (Original) The method of claim 6 wherein halting programs not needed by said security module while said password entry screen is displayed comprises inhibiting context-switching by an operating system in said computing device to programs not needed by said security module.

9. (Original) The method of claim 6 wherein halting programs not needed by said security module while said password entry screen is displayed comprises:

storing a status table in random access memory used by an operating system in said computing device, each entry in said status table relating to a currently executing program and containing a status indication associated with said currently executing program;

saving current settings of said status table; and

changing said current settings so as to inhibit execution by said operating system of said programs not needed by said security module.

10. (Original) The method of claim 6 wherein halting programs not needed by said security module while said password entry screen is displayed comprises:

storing an alternate status table in random access memory used by an operating system in said computing device, each entry in said alternate status table relating to a program needed by said security module;

instructing said operating system to use said alternate status table while said password entry screen is displayed.

11. (Original) A device for inputting a confidential password comprising:

a secure processor executing a password program to obtain a password from a user;

memory operatively connected to said secure processor storing authentication indicia recognized by a user of said device;

a display operatively connected to said secure processor to display a password entry screen containing said authentication indicia.

12. (Original) The device of claim 11 further comprising a smart card containing said secure processor and said memory.

13. (Original) The device of claim 11 further comprising a security lock program executed by said secure processor to inhibit execution of programs not needed by said secure processor to obtain said password from said user.

14. (Original) The device of claim 13 wherein said security lock program inhibits an operating system from responding to interrupts not associated with said secure processor while said password entry screen is displayed.

15. (Original) The device of claim 13 wherein said security lock program inhibits an operating system from context-switching while said password entry screen is displayed.

16. (Original) The device of claim 13 wherein said security lock program inhibits execution of programs not needed by said secure processor to obtain said password from said user.

17. (Original) The device of claim 16 wherein said security lock program inhibits execution of programs not needed by said secure processor to obtain said password from said user by changing settings in a status table used by an operating system while said password entry screen is displayed.

18. (Original) The device of claim 16 wherein said security lock program inhibits execution of programs not needed by said secure processor to obtain said password from said user by causing an operating system to use an alternate status table while said password entry screen is displayed.

19. (Original) A device for a performing secure transactions, said device comprising:

memory storing authentication indicia recognized by a user of said device;

a secure processor programmed to:

prompt said user to enter a password by displaying a password entry screen containing said authentication indicia; and

perform said secure transaction following entry of said password by said user.

20. (New) The device of claim 19 wherein said secure processor and said memory are contained within a removable security module.

21. (New) The device of claim 20 wherein said removable security module comprises a smart card.